(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 October 2002 (03.10.2002)

PCT

(10) International Publication Number
WO 02/078286 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/US02/09504

(22) International Filing Date: 27 March 2002 (27.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/279,041 27 March 2001 (27.03.2001) US
Not furnished 27 March 2002 (27.03.2002)

(71) Applicant: BEA SYSTEMS, INC. [US/US]; 2315 N. First Street, San Jose, CA 95131 (US).

(72) Inventor: MOSES, Fred; ** (US).

(74) Agent: HAMILTON, John, A.; Choate, Hall & Stewart, Exchange Place, 53 State Street, Boston, MA 02109 (US).

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

**Published:**
— *without international search report and to be republished upon receipt of that report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: SYSTEM AND METHOD FOR MANAGING OBJECTS AND RESOURCES WITH ACCESS RIGHTS EMBEDDED IN NODES WITHIN A HIERARCHICAL TREE STRUCTURE

(57) Abstract: A system and method for controlling access to data within a hierarchically organized document, such as an XML document. Elements may have their access rights specified, for example as a variable in an XML tag. If not specified within an element of the document, access rights are inherited from its nearest ancestor. Specified access rights may refer to a collection of entitlement expressions, which describe with arbitrarily fine granularity which users and user types may access the data.

EntitlementIDs:
<entitlementID ID="E1" V="doctors+nurses"/>
<entitlementID ID="E2" V="lab techs"/>

XML text:

```
<A entitlement="E1">
    <B> ... </B>
    <C entitlement="E2">
        <D> ... </D>
    </C>
</A>
```

| Element | Entitlement |
|---|---|
| A | E1 |
| B | E1 |
| C | E2 |
| D | E2 |

WO 02/078286 A2

# System and Method for Managing Objects and Resources with Access Rights Embedded in Nodes Within a Hierarchical Tree Structure

The present application claims benefit of U.S. Provisional Application No. 60/279,041, filed March 27, 2001, which is incorporated herein by reference.

## Field of the Invention

The present invention provides a system and method for managing objects and resources with access rights embedded in nodes within a hierarchical tree structure. The system is suitable for implementation of HL7-approved XML standards for medical records and/or messages.

## Background of the Invention

Controlling the access of a large number of users to a vast array of data represents one of the greatest challenges facing the future of the Internet. One example of an immense access control undertaking that will exceed the capabilities of current access control systems relates to the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA will be implemented in accordance with a Rule (Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations p. 82462, 45 CFR Parts 160 and 164, Rin: 0991–AB08, Standards for Privacy of Individually Identifiable Health Information) promulgated by the Department of Health and Human Services (HHS) in an effort to achieve the adoption of industry standards for the electronic transmission of health information. In short, HIPAA requires that all patient information transfers between organizations be in a standardized form and that standards of privacy be maintained. Health Level 7 (HL7) is an organization that creates the standards for storage and interchange of medical records encompassed by HIPAA. Standardization complications include the fact that there are currently about 400 formats for electronic health care claims processing in use nationwide. Further, the need to manage this information will require finely granular (down to the per field

level) access to a massively scaled number of records. This access must obey the mandated confidentiality and respect specific patient confidentiality requests.

HL7 has chosen the eXtensible Markup Language (XML) as the basis for structuring medical records for storage and messaging. This language organizes data as a tree structure documents. XML is standardized by W3C, (http://www.w3.org/TR/REC-xml ). W3C is an international industry consortium responsible for developing common code standards for the World Wide Web.

Applications storing or transferring medical records will require access control mechanisms to assure that HIPAA requirements are met. It is an object of the present invention to supply this need.

U.S. Patent No. 6,061,684, "Method and system for controlling user access to a resource in a networked computing environment," assigned to Microsoft Corporation (Redmond, WA), describes a unified and straightforward approach to managing file and other resource security in a networked computing environment. The invention can be implemented in a multi-user computer network that includes a client computer, a server computer that controls a resource sharable among users of the network, such as a shared file folder or directory, and a communications pathway between the client computer and the server computer. The resource is organized as a hierarchy of elements with a root element at the top of the hierarchy and additional elements below the root element. According to the invention, a request is received to change a protection, such as an access permission, of an element of the resource hierarchy (other than the root) with respect to a particular network user. If the element in question lacks an associated access control list, a nearest ancestor element of the hierarchy is located that has an associated access control list. The first (descendant) element inherits the access control list of the second (ancestor) element. This inheritance is done by generating a copy of the access control list of the second element and associating the generated copy with the first element. The requested change in protection is then incorporated into the generated copy that has been associated with the first element so as to establish an updated access control list for the first element. Further, the requested change can be propagated downwards in the hierarchy from the first element to its descendants having access control lists.

U.S. Patent No. 6,038,563, "System and method for restricting database access to managed object information using a permissions table that specifies access rights corresponding to user access rights to the managed objects," assigned to Sun Microsystems, Inc. (Palo Alto, CA), describes an access control database that specifies access rights by users to specified sets of the managed objects. The specified access rights include access rights to obtain management information from the network. An access control server provides users access to the managed objects in accordance with the access rights specified by the access control database. An information transfer mechanism sends management information from the network to a database management system (DBMS) for storage in a set of database tables. Each database table stores management information for a corresponding class of managed objects. An access control procedure limits access to the management information stored in the database tables using at least one permissions table. A permissions table defines a subset of rows in the database tables that are accessible to at least one of the users. The set of database table rows that are accessible corresponds to the managed object access rights specified by the access control database. A user access request to access management information in the database is intercepted, and the access control procedure is invoked when the user access request is a select statement. The database access engine accesses information in the set of database tables using the permissions tables such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access.

U.S. Patent No. 5,878,415, "Controlling access to objects in a hierarchical database," assigned to Novell, Inc. (Provo, UT), describes methods and systems for controlling access to objects in a hierarchical database. The database may include a directory services repository, and/or synchronized partitions. An access constraint propagator reads an access control property of an ancestor of a target object. The access control property designates an inheritable access constraint such as an object class filter or an "inheritable" flag. The object class filter restricts a grant of rights to objects of an identified class. The "inheritable" flag allows inheritance of an access constraint on a specific object property. The propagator enforces the inheritable access constraint by applying it to at least the target object.

## Summary of the Invention

In one aspect, the present invention comprises a system for managing objects and resources with access rights embedded in nodes within a hierarchical tree-structure. The system includes a host, housing a Web server, a database server, an entitlement server, and a transaction server; a network, such as the Internet or an intranet; and one or more client PCs.

In another aspect, the present invention comprises a method of inputting a transaction in XML form for use in the determination and granting of access rights embedded in nodes within a hierarchical tree structure. The method includes receiving transaction data from the external system; parsing and validating the XML; determining whether the received data is valid; adding access data to the entitlement server and text content to the database server; determining whether an error occurred; sending an error message to the external system; and sending a confirmation message to the external system.

In yet another aspect, the present invention comprises a method of interacting with a host system into which an XML document has been accepted. The method includes identifying the user accessing the host using a client PC; receiving a request; determining whether an access check is needed; determining whether permission should be granted; performing the request; replying to the user; and handling the denial of the request.

One advantage of the present invention is that it provides a way to protect objects described by a tree structure.

A second advantage of the present invention is that it provides a way to protect objects with as much granularity as the tree structure permits.

A third advantage of the present invention is that it provides a way to protect objects with as much granularity as the set of users permits.

A fourth advantage of the present invention is that the entitlement IDs (or expressions or objects) can be defined in a diverse ways, allowing for a wide variety of applications.

A fifth advantage of the present invention is that the entitlement IDs may be collected separately, meaning that they do not need to be sprinkled throughout the

code structure. They can be cached before the XML is parsed, leading to improved system speed and efficiency.

A sixth advantage of the present invention is that may be packaged either as a separate XML document or as a separate part of the document containing the objects to protect.

## Brief Description of the Drawing

The invention is described with reference to the several figures of the drawing, in which,

**Figure 1** shows a system for managing objects and resources in a hierarchy with access rights embedded in nodes;

**Figure 2** is a flow chart illustrating a method of inputting a transaction in XML form;

**Figure 3** is a flow chart illustrating a method of interacting with a host system into which the XML document has been accepted; and

**Figure 4** illustrates the used of XML to manage objects and resources in a hierarchy with access rights embedded in some nodes.

## Detailed Description

**Figure 1** illustrates a system for managing objects and resources in a hierarchy with access rights embedded in nodes. System **100** includes a host **105**, comprising a Web server **110**, a database server **120**, an entitlement server **130**, and a transaction server **140**, which are all interconnected within host **105**. Host **105** can be either a single computer, or a series of computers operating in concert. System **100** also includes connections to a network **150** (such as the Internet or an intranet), through which an external system **160**, and one or more client PCs **170** connect with host **105**.

In some embodiments of the invention, external system **160** and client PCs **170** use network **150** to communicate with host **105** for the purposes of generating and receiving documents programmed in XML. In other embodiments, client PCs **170** need never actually create or access XML directly. Instead, web server **110** invokes transaction server **140** to request text from an XML document, and then transforms the text into HTML to send back to the client PC **170**.

Typically, client PC **170** is a personal computer. External system **160** may be a peer to host **105** or a host-type system of wholly separate elements; however, external system **160** must contain an application capable of generating and translating XML. Host **105** represents a network-connected host environment consisting of one or more servers. Web server **110**, which may be a single server or multiple servers operating in a cluster, executes the functions associated with serving World Wide Web pages. Database server **120** stores the actual content of the XML transactions and is called upon by other elements of host **105** for such content. The internal form of the content need not be XML as long as the tree structuring information is preserved. Entitlement server **130** operates as one type of a database server dedicated to hosting and adjudicating access control for applications served by host **105**. The functionality of one suitable entitlement server **130** is fully described in U.S. Patent 6,154,741 to Feldman, which is assigned to EntitleNet, Inc., and incorporated herein by reference. Transaction server **140** functions as the XML interpreter, and houses various software applications for that purpose, including those that pass portions of submitted XML documents to entitlement server **130** and database server **120** for storage. Transaction server **140** also receives transaction results from entitlement server **130** and database server **120** and responds accordingly to the transaction's requestor. In addition, transaction server **140** governs the retrieval of requested portions of XML documents.

**Figure 2** is a flowchart illustrating a method of inputting a transaction in XML form. Entitlement information within the XML affects the exchange with respect to the way permission to access information is granted. Method **200** includes the following steps:

*Step 210: Receiving transaction data*

In this step, transaction server **140** receives an XML document with associated transaction data generated by external system **160**. External system **160** sends this XML document to transaction server **140** via network **150**.

*Step 220: Parsing and validating XML*

In this step, transaction server **140** parses the received XML document to check for validity using software applications and techniques well known in the art.

*Step 230: Are the data valid?*

In this decision step, transaction server **140** determines whether the XML document is valid. If yes, process **200** proceeds to step **240**; if no, process **200** proceeds to step **260**.

*Step 240: Adding access data to entitlement server and text content to database server*

In this step, transaction server **140** translates the information parsed in step **220** into the appropriate internal form and stores it on entitlement server **130** and database server **120**. In particular, access information is added to entitlement server **130**, and the text information is saved to database server **120**. In addition, some tracking information is added to database server **120** to track the processing performed.

*Step 250: Did an error occur?*

In this decision step, transaction server **140** checks to see if any errors occurred thus far. If yes, process **200** proceeds to step **260**; if no, process **200** proceeds to step **270**.

*Step 260: Sending error message*

In this step, transaction server **140** sends an error message back to the originating external system **160** via network **150**, and processing ends.

*Step 270: Sending confirmation message*

In this step, transaction server **140** sends a confirmation message back to originating external system **160** via network **150**, and processing ends.

**Figure 3** is a flowchart illustrating a method of interacting with a host system into which the XML document has been accepted. While **Figure 2** covered the programmatic interface with host **105** using external system **160**, **Figure 3** instead covers the interaction of client PCs **170** with host **105**. Method **300** includes the following steps:

*Step 310: Authenticating user*

In this step, Web server **110** authenticates users on client PC **170** talking to host **105** using network **150** and applications known in the art, such as using a secure socket layer interchange.

*Step 320: Receiving request*

In this step, Web server **110** receives a request for information from a user using Web-browsing software installed on client PC **170**.

*Step 330: Is an access check needed?*

In this decision step, Web server **110** determines whether the information request requires an access control check. If yes, process **300** proceeds to step **340**; if no, process **300** proceeds to step **380**.

*Step 340: Is permission granted?*

In this decision step, entitlement server **130** determines whether to grant access based on user identification obtained in step **310** and the access check performed in step **330**. If yes, process **300** proceeds to step **350**; if no, process **300** proceeds to step **370**.

*Step 350: Performing request*

In this step, entitlement server **130** performs the request received from Web server **110**. The performance of this request (or adjudication) is fully described in U.S. Patent 6,154,741 assigned to EntitleNet, Inc.

*Step 360: Replying to user*

In this step, Web server **110** sends a reply to the request for information originating from client PC **170** via network **150**, and processing ends.

*Step 370: Handling denial*

In this step, Web server **110** handles the denial of access to information (i.e., the user on client PC **170** is not allowed to receive the information requested) by communicating with client PC **170** via network **150**, and processing ends.

**Figure 4** illustrates the use of XML to manage objects and resources in a hierarchy with access rights embedded in some nodes. An **entitlementID** element creates a BMAP object with a name given by the **ID** attribute and entitles it with the entitlement expression given by the **V** attribute. (The names are arbitrary and chosen for the purposes of exposition.) An arbitrary number of these may be defined to yield any desired granularity.

An **entitlement** attribute within an element specifies the **entitlementID** governing the element. Entitlements are enforced in a tree-oriented manner with lower or enclosed elements of the tree governed by the enclosing nodes. An exception to this is that an **entitlement** attribute on an element supercedes the entitlement of higher nodes. This presents two constructs which, when used in concert, allow the specification of the control of access to portions of an XML data structure.

Other embodiments of the invention will be apparent to those skilled in the art from a consideration of the specification or practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with the true scope and spirit of the invention being indicated by the following claims.

What is claimed is:

1. A method of controlling access to a hierarchically organized collection of data elements, comprising:

examining in succession a data element and optionally one or more ancestor elements of the data element to determine an entitlement status for the element;

consulting an entitlement ID to determine an entitlement group corresponding to the entitlement status;

consulting a membership map to determine whether a selected user is a member of the entitlement group, wherein the membership map comprises a matrix of users and group memberships; and

allowing the user to access the data element only if the user is a member of the entitlement group.

2. The method of claim 1, wherein the membership map is stored as a bit map.

3. The method of claim 1, wherein the entitlement status in the data element or ancestor element is an entitlement expression.

4. The method of claim 1, wherein the hierarchically organized collection of data elements is an XML document.

5. The method of claim 4, wherein the XML document complies with the HIPAA standard.

6. The method of claim 1, further comprising caching entitlement group definitions for the hierarchically organized collection of data elements prior to consulting the membership map.

7. Method of describing access restrictions on individual elements of a document having a hierarchical structure, comprising:

placing entitlement ID's in one or more elements of the document, said entitlement ID's referring to entitlement expressions describing classes of users allowed to access the elements, where the entitlement ID

applicable to an element is the ID placed in the element or in the first ancestor of the element having an entitlement ID.

8. The method of claim 7, wherein the document is an XML document.

9. The method of claim 8, wherein the entitlement ID's are variable settings on XML tags.

10. The method of claim 8, wherein the XML document complies with HIPAA standards.

11. The method of claim 7, wherein the document comprises a table of entitlement ID's and corresponding entitlement expressions.

12. A method of providing a document having access restrictions described according to the method of claim 7, comprising:
consulting the entitlement ID's and comparing them with entitlement groups of the user; and
serving to the user those portions of the document which the user is authorized to receive.

13. The method of claim 12, wherein user authorizations are stored in a membership map.

14. The method of claim 13, wherein the membership map is a bit map.

15. The method of claim 12, further comprising caching entitlement expressions in the document prior to serving to the user.

16. A system for providing information to users selectively according to predetermined access rights, the system comprising:
a database of records, the records being hierarchically organized into elements, at least some the elements comprising access rights information;
an entitlement server comprising a membership map describing user membership in access groups; and

a transaction server that consults the database and the entitlement server and serves information to users in response to requests only if users are allowed to access the information.

17. The system of claim 16, wherein the records are XML documents.

18. The system of claim 17, wherein the XML documents comply with HIPAA standards.

19. The system of claim 16, wherein access rights to an element are controlled by access rights information embedded therein if such access rights information exists, and by access rights information embedded in the first ancestor element having such access rights information if the element does not comprise embedded access rights information.

20. The system of claim 16, wherein the access rights information is an entitlement expression.

21. The system of claim 16, wherein the membership map is a bit map.

22. The system of claim 16, wherein the transaction server serves an XML document comprising only elements for which the user has access rights.

23. The system of claim 16, wherein the transaction server uses an XML document having access rights information embedded therein to build an HTML document comprising only elements for which the user has access rights, and serves the HTML document to the user.

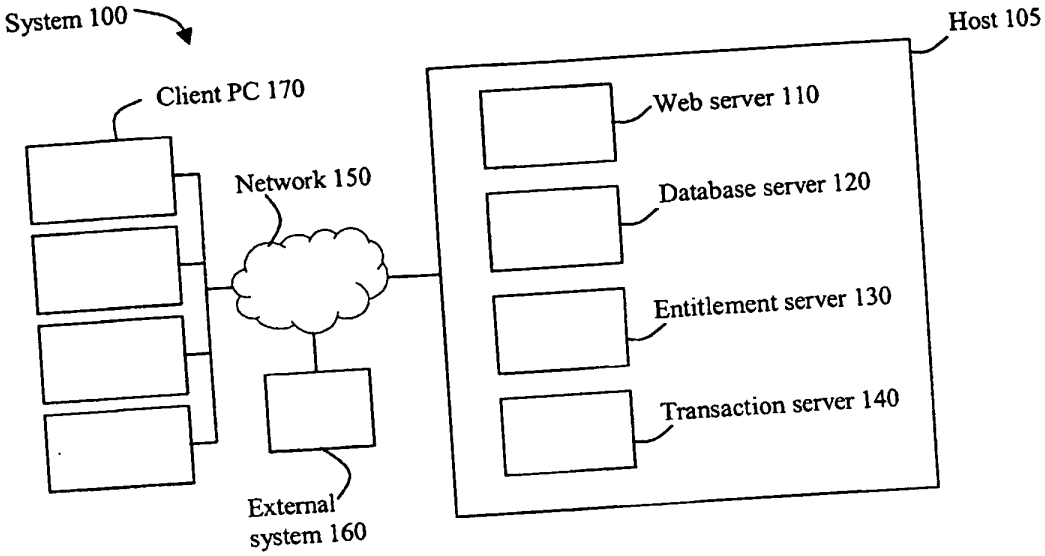
System 100
Client PC 170
Network 150
External system 160
Host 105
Web server 110
Database server 120
Entitlement server 130
Transaction server 140

**Figure 1**

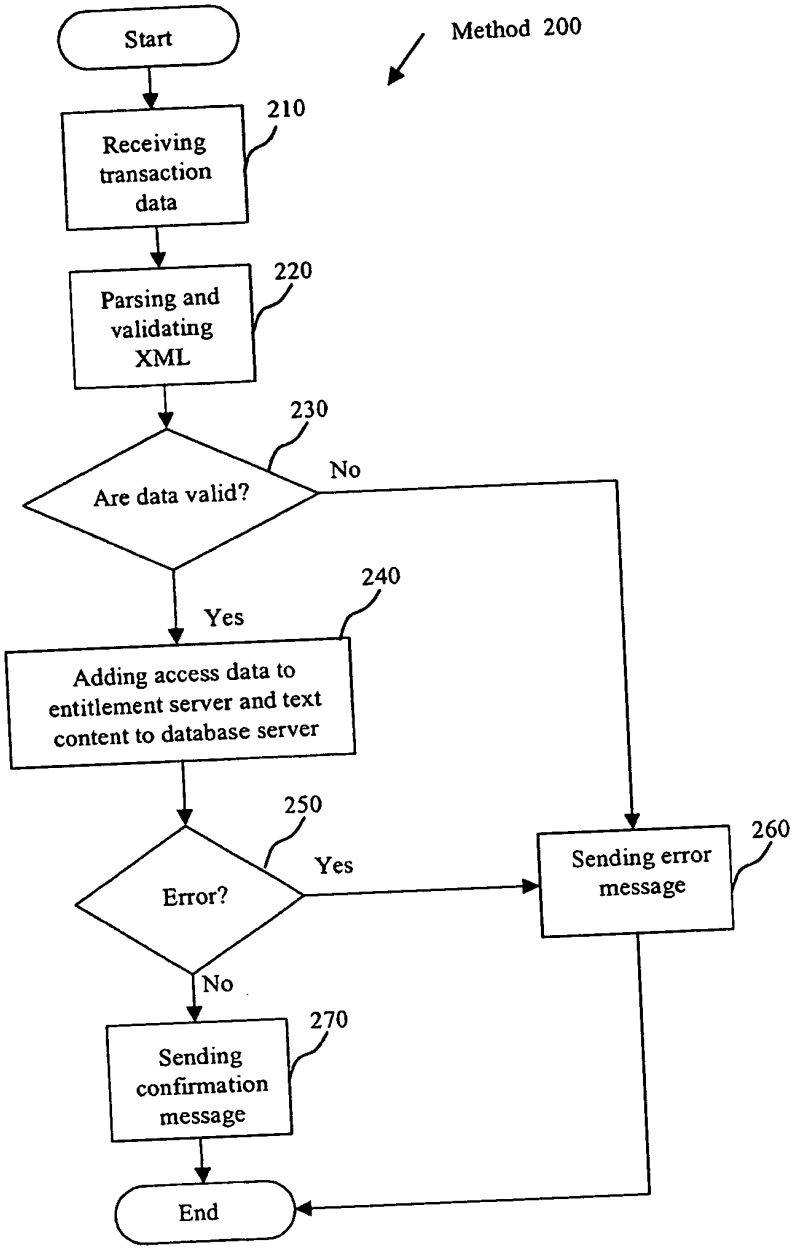
Start
Method 200
Receiving transaction data
210
Parsing and validating XML
220
Are data valid?
230
No
Yes
Adding access data to entitlement server and text content to database server
240
Error?
250
Yes
Sending error message
260
No
Sending confirmation message
270
End

**Figure 2**

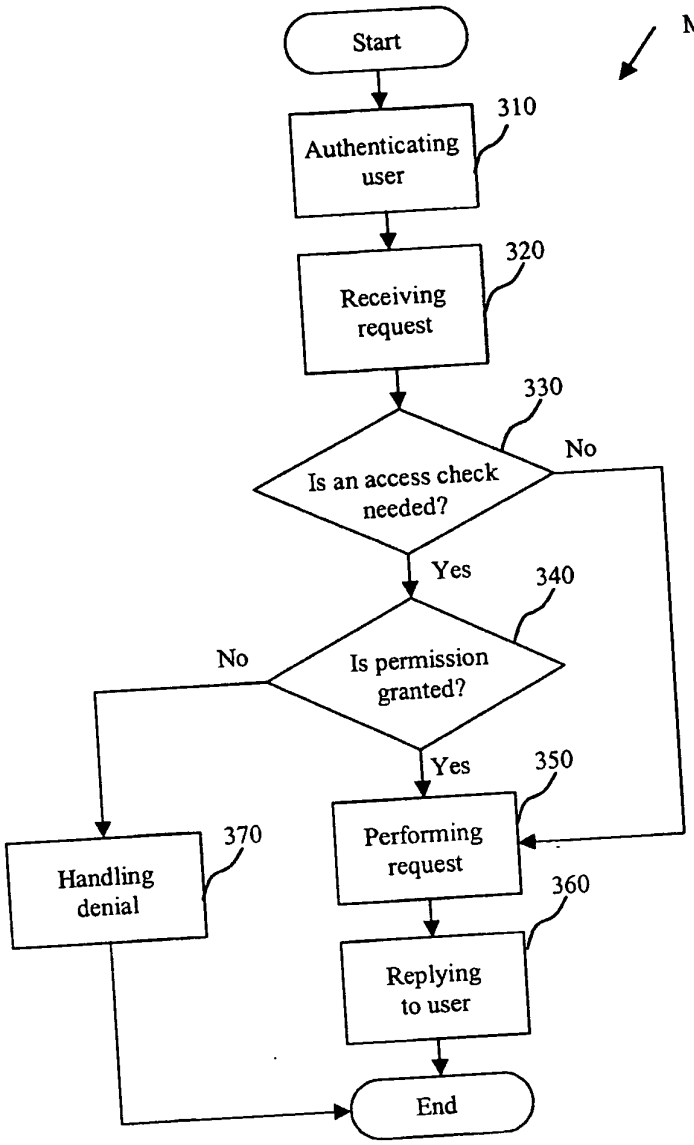
Method 300
Start
Authenticating user
310
Receiving request
320
Is an access check needed?
330
No
Yes
Is permission granted?
340
No
Yes
Performing request
350
Handling denial
370
Replying to user
360
End

**Figure 3**

EntitlementIDs:

<entitlementID ID="E1" V="doctors+nurses"/>

<entitlementID ID="E2" V="lab techs"/>

XML text:

```
<A entitlement="E1">
    <B> ... </B>
    <C entitlement="E2">
        <D> ... </D>
    </C>
</A>
```

| Element | Entitlement |
|---|---|
| A | E1 |
| B | E1 |
| C | E2 |
| D | E2 |

**Figure 4**